>> John Mellen, a detective in the Louisville Metro Police Department's Financial Crimes Unit, immediately contacts the victim to begin his identity theft investigation. Though the initial incident report has already been taken on the identity theft before the case is assigned to Detective Mellen, he contacts the victim to get as much pertinent information from the individual about the thefts as possible, including how they found out about the identity theft, he said.

The ITRC recommends that law enforcement agencies develop an identity theft victim guide that outlines the steps victims should take to prepare for the investigator's phone call or visit. The guide, given to victims when the initial incident report is filed, will help them organize their thoughts in order to speak clearly and concisely about the incident. It also gives victims the opportunity to get started immediately, fulfilling an emotional need for them, as well.

In that initial correspondence, Mellen said he encourages victims to keep a detailed account of every step of the investigation.

"What I generally tell people is … to keep the report number handy and create a file for themselves," he said. "With that file they'll keep a notebook and write down every correspondence they have with anybody, to include this one — starting right today with me speaking to them — with a date and time stamp."

Once all the information is collected from the victim, the claim is then thoroughly researched. Sometimes cases can be rather simple if the victim knows or has an idea who the suspect is.

"Sometimes they'll know and say, 'My sister stole my identity and put her cable or [electric] bill in my name and she lives at this address,' so you subpoena the records from [those companies] and research the suspect and … go out there and actually find them," Mellen said.

Between 70 and 80 percent of all identity theft cases are someone close to the victim, Mellen said. But the remaining 20 to 30 percent, where the perpetrator is a complete stranger, are much more difficult to work.

"It's finding that person initially that's the tough part," Mellen said. "With those it's just more in depth because you have to go back, and you really have to rely on the victim to give you the records you need, like the credit report."

"The big thing is we have to know where it originated from," Raup said. "The first thing we need to know is how was this account set up — 90 percent of the time it was done online."

Once it is determined how the individual was victimized, records can be subpoenaed. For example, if a credit card was fraudulently set up in the victim's name, then subpoenaed records from the credit card company may help trace the original Internet Protocol or IP address from which the credit card was applied. Then records from that Internet provider may provide a lead to a specific address or user that may be the suspect — but it is not always that simple.

"Nine times out of 10 it's not local," Raup said. "Most of the time when we resolve one back like that, it's from somewhere else and we usually cannot figure out how and when they got [the individual's information]. More than likely they didn't even get it, but bought it from someone else."

Stealing identities for the purpose of selling them online to others for creating fake identities has become a business in today's high-tech, information-privileged society.

"If someone wants, they can pay a small fee and can pull up anything they want on people through public records," Hopkinsville's Finley said. "There's definitely enough information available out there to steal an identity.

"The biggest distributors of false or pharmed information for use in identity theft are off shore, out of the country — and we can't touch them," he continued. "What we advise at that point is mostly damage control."

FOLLOWING THE PAPER TRAIL

Since there are so many methods identity thieves can use to steal an identity and the places they find that information are just as numerous, it is vital that law enforcement officers be aware of what kind of evidence is out there to help them investigate their cases. In financial identity theft, items such as application forms, signature cards from a checking account, records of calls made from a specific telephone number, shipping records, videotapes from security monitoring systems and bankruptcy records could hold critical evidence to help solve the case as quickly as possible. For example, the checking account withdrawal signature can provide proof that the signature on the form is not that of the victim. Also, these records can show trends, provide names and addresses where merchandise was shipped, provide potential witnesses and help pinpoint the possible location of the imposter.